審査の結果の要旨

氏名　　松田　隆宏

本論文は、「Security Notions and Generic Constructions of Chosen Ciphertext Secure Public Key Encryption Schemes（選択暗号文攻撃に対して安全な公開鍵暗号の安全性定義と一般的構成法）」と題し、汎用的に用いられる場合は必須とされる選択暗号文攻撃に対する安全性（CCA 安全性）を持つ公開鍵暗号方式の一般的構成法として、実用的な効率を持つ具体的方式につながる構成法を提案し、さらに、CCA 安全な公開鍵暗号が存在するための必要十分条件に関して深く詳細に論じる新たな理論体系を示している。論文の構成は、「Introduction」と「Basic Definitions」を含め５章からなる。

第 1 章は「Introduction（序論）」で、本研究の背景と動機を述べ、成果の概要をまとめている。特に、CCA 安全性の重要性と、CCA 安全性を持つ公開鍵暗号方式を他の要素技術の組み合わせで構成する一般的構成法に関する重要な２つの未解決問題について、述べている。１つは実用的な具体的方式につながる一般的構成法は可能かという問題であり、もう１つは、公開鍵暗号として最低限の安全性である選択平文攻撃に対する安全性（CPA 安全性）しか持たない方式のみを用いて CCA 安全な公開鍵暗号方式を構成できるかという問題である。本章では、暗号理論におけるこれらの未解決問題の重要性から、本研究を行う意義を明らかにしている。

第 2 章は「Basic Definitions（基本的な定義）」と題し、暗号技術一般の証明可能安全性について、次章以降で用いられる各要素技術の機能的要件と安全性要件を厳密に記述している。

第 3 章は「Practical Constructions: IBE-to-PKE Transformations（実用的な構成法: IBE-to-PKE 変換）」と題し、CCA 安全性と実用的な効率を持つ具体的な公開鍵暗号方式をもたらす一般的構成法を目指し、IBE-to-PKE 変換と呼ばれるタイプの一般的な構成法を二種提案している。ID ベース暗号（IBE）とは、公開鍵暗号のうちで任意の文字列を公開鍵とできる特殊なクラスであり、IBE-to-PKE 変換とは、CPA 安全性しか持たない IBE を CCA 安全な公開鍵暗号へ変換する手法である。第一の提案では、CPA 安全性よりもやや強い安全性である頑強性を IBE に要求することで、IBE 以外の要素技術として、最も基礎的な要素技術である一方向関数のみしか使用しない非常に簡素な変換を実現している。第二の提案では、Encapsulation と呼ばれる特殊なコミットメント方式の効率的な構成法を示し、それを用いて従来の IBE-to-PKE 変換を効率化できることを示している。両提案手法では、IBE として実用的な効率を持つ方式を用いれば変換後の公開鍵暗号も実用的な効率を持つという点で、従来の IBE-to-PKE 変換が抱えていた非効率性の課題を克服している。

第 4 章は「Towards CCA Security from CPA Security（CPA 安全性から CCA 安全性へ向けて）」と題し、CPA 安全な公開鍵暗号のみを用いて CCA 安全な公開鍵暗号を構成できるかと

いう、暗号理論における極めて重要な未解決問題に取り組んでいる。本章では最初に、既存研究よりも深く詳細に構成可能性及び構成不可能性を議論するためにはCPA安全性とCCA安全性の間に位置する安全性を定義するのが有効であることを指摘し、「Mixed CCA安全性」を新たに定義している。この安全性は、単一型と並行型の復号クエリを事前に決められた順序で行う攻撃者に対する安全性であって、攻撃者に許される行為を詳細かつ厳密に捉えるという暗号理論の真髄を高いレベルで追究した成果であり、理論体系の基盤となる。実際、本章では、Mixed CCA安全性において表現できる安全性定義間の包含や隔離の関係を完全に解明する定理の導出に成功している。さらに、従来の構成法が達成した安全性よりも真に強い安全性、及び、従来の構成では達成されていない種類の安全性を持つ公開鍵暗号の、CPA安全な公開鍵暗号のみを用いた構成法を示している。本章の最後では、さらなる理論的発展をもたらすための示唆として、Mixed CCA安全性に関する未解決問題についても議論している。

最後に第5章は「Conclusion（結論）」で、本研究の総括を行い、併せて将来展望などについて述べている。

以上これを要するに、本論文は、CCA 安全性を持つ公開鍵暗号の一般的構成法に関して、実用的な具体的方式につながる構成法や、CPA安全な方式のみから構成することの可能性及び不可能性を論じるための理論基盤を、厳密な証明可能安全性の枠組みで体系的に示した論文であり、電子情報学、特に情報セキュリティ工学上貢献するところが大きい。

よって本論文は博士(情報理工学)の学位請求論文として合格と認められる。